The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

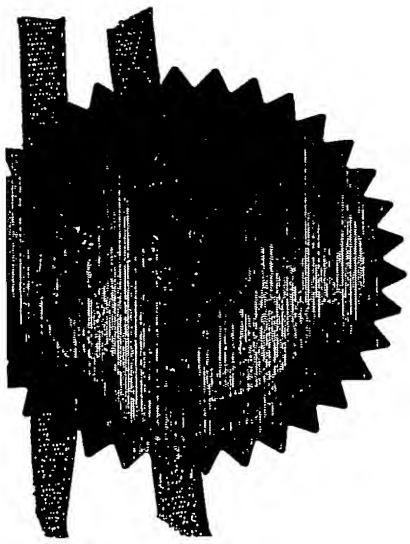
I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears an amendment, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed J Evans.

Dated 28 March 2003

Patents Form 1/77

...ts Act 1977
...16)

THE PATENT OFFICE
G
0 8 MAR 2002
NEWPORT

The Patent Office

GBAR02 E701632-1 D01038
P01/7700 0.00-0205459.1

1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office
Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — KRT/P302995GB

2. Patent application number *(The Patent Office will fill in this part)* — 0205459.1 — 8 MAR 2002

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

First 4 Internet Ltd
6 South Bar Street
Banbury
Oxon
OX16 9AA
United Kingdom

Patents ADP number *(if you know it)* — 8340085001

If the applicant is a corporate body, give the country/state of its incorporation — A British company

4. Title of the invention — Data Protection System

5. Name of your agent *(if you have one)*
"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

~~WITHERS & ROGERS~~ R.G.C Jenkins & Co
~~Goldings House~~ 26 Caxton Street.
~~2 Hays Lane~~ London
~~London~~ SW1H 0RJ.
~~SE1 2HW~~

Patents ADP number *(if you know it)* — ~~1776001~~ 03966736001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	10
Claim(s)	3
Abstract	1
Drawing (s)	-

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature Withers & Rogers WITHERS & ROGERS Date 8 March 2002

12. Name and daytime telephone number of person to contact in the United Kingdom

Keith Tart 0121 245 3900

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least six weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500 505.*
b) *Write your answers in capital letters using black ink or you may type them.*
c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*
d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*
e) *Once you have filled in the form you must remember to sign and date it.*
f) *For details of the fee and ways to pay please contact the Patent Office.*

Data Protection System

This invention concerns apparatus, methods and articles manufactured thereby for preventing theft of copyright material, particularly as recorded in digital form on carrier means such as optical disc media. In this description optical disc media is intended to include not only CDs, CD-ROMs and DVDs, but also similar media that may be read using electromagnetic radiation outside of the visible range; for example, infra-red, ultra-violet or X-rays.

The advent of recordable CDs (CD-R) has made it generally easy and inexpensive to make unauthorised copies of Audio CDs and CD-ROMs; for example by copying the entire contents of a audio CD to a computer hard disc and then writing this to a CD-R. The potential loss of revenue to recording companies from such activities is considerable, and indeed its impact has already been felt. Consequently, there has been much interest in techniques that prevent such unauthorised copying.

US 5513260 (Ryan) and US 5659613 (Copeland) disclose a method of placing an authenticating signature on a legitimate copy that cannot easily be detected, and hence transferred to an illicit copy. New CD players would need a subsystem that searched for such a signature and if the signature should be there, but was not found, refuse to play the disc.

US 20010054028 A1 (Kuroda) describes the addition of copy control information to copyright material, such that when an attempt is made to copy this material using reproduction and recording apparatus according to the invention such copying is prevented, if appropriate, on the basis of the copy control and information and also attribution information generated by the reproduction apparatus.

US 2002003880 A1 (Kato) discloses a system where a recording of copyright material is encrypted and also has a digital watermark which is read by apparatus according to the invention, thereby allowing the replay apparatus to obtain a disk key and so decrypt the material.

All of the above methods and systems suffer from the disadvantage that they do not prevent unauthorised copying of a CD and replay of that copy on most existing CD players; that is they require new players equipped with appropriate hardware.

US 20020001690 A1 (Selinfreund) discloses a method of manufacturing optical discs that includes areas on the disc with light-sensitive material. During the first pass of a conventional optical reader the digital information on such light sensitive areas is read correctly, but on a second pass the data is read differently due to the activation of the light sensitive material by the optical reader As most optical disc readers and players are pre-programmed to re-sample data areas to assure correct copying such discs will fail to copy correctly. While this method will work with many existing players, the inclusion of light sensitive areas at precise locations on the disc is expected to significantly increase disc production costs.

US 20010053979 A1 (Kori) describes an encryption protection system that encrypts copyright material, requiring the user to have the decrypting key, and also keeps a record of the number of copies made, so that a pre-determined limit can be placed on this. However, determined copyists can with sufficient effort break such a single or double key systems. Further, this system appears unsuitable for replaying discs in most currently available players.

An object of some aspects of the present invention is to provide improved methods of protecting copyright digital data recorded on a data storage medium, particularly optical discs such as CDs. It is a further object of some

aspects of the invention to provide a method of producing optical discs that provide such improved protection. It is also an object of some aspects of the present invention to provide an optical disc with such improved protection. A further object of some aspects of the invention is to provide a system that is effective when used with most players and computers presently available.

CD audio discs contain at least a first session formatted in compliance with the well known "Red Book", also known as standard 908 of the International Electrotechnical Commission (IEC) entitled "Compact Disc Digital Audio System" (Geneva, Switzerland, 1987).

According to one aspect of the invention slight deviations from strict "Red Book" compliance are introduced into this first session to prevent most CD-ROM drives reading the data. Thus, the first session on the disc will normally contain audio tracks. In the lead in area of the disc, the Q-channel information contains the Table of Contents (TOC). Each audio track on the first session is described in the TOC including where the track is located on the disc and the type of track. In a conventional CD the tracks are described as audio tracks. In a disc according to the invention such audio tracks are described as data tracks in the TOC. A normal CD player does not reference this TOC but rather looks at Q-channel data in each sector within the session. This track area data is unaltered and conforms entirely to "Red Book" standard. Hence, such a disc will play normally in a standard "Red Book" audio CD player. However, when such a disc is read by a CD-ROM drive the drive will reference the TOC and will then recognise a discrepancy between the TOC data and that Q-channel data within each sector of the track. This contradiction normally results in an "illegal mode for this track", that prevents the CD-ROM drive reading the track.

Specifically, the TOC describes the tracks in the audio session as data tracks, control = 4 (0100 binary). Normally they would be described as audio tracks, control = 0 (0000 binary) (see "Red Book", p41).

No amendments are made to the well known Cross Interleave Reed-Solomon Code (CIRC) error protection data on the protected disc.

A further important aspect of the invention is the ability to play the optical disc on a computer. This is achieved by first compressing the audio tracks, then encrypting this data and recording this resulting data in a second session on to the optical disc, known as a data session.

For a CD this data is recorded in the following manner; the data is first split into logical block that will fit into a "Yellow Book" (IEC) standard CD sector (also known as a logical block). Each of these blocks is then encrypted using an encryption key derived from its logical block address (LBA) or position on the CD. The data resulting from this process is then written to the disc at this position (LBA) using conventional mastering and recording methods. This compressed audio data is not visible to the host computer under normal circumstances. The data is played on a personal computer, by including in this second session a "CD player application program" that is visible to the host computer. This player has built into it the ability to locate, decrypt and play the compressed and encrypted audio data.

To enable protected discs to be played on computers using operating systems such as Windows 95, 98, NT-4, 2000ME, 2000 Professional, 2000 Server, 2000 Server Professional, XP Home Edition, XP Professional, Linux 6.2 and higher, Apple Macintosh OS9 and higher, Sun Unix OS8; hereafter referred to as PCs, at least one further data session is included on the disc.

This further session is located after the first "Red Book" compliant session and conforms to the IEC "Yellow Book" standard and the IEC "Orange Book" standard for multi-sessions. This session contains the player application program and any associated files, which are visible to the computer operating system and also encrypted data files containing the audio tracks; these latter files not being visible to the computer operating system or playable, except by using the CD player application program provided on the disc.

Thus, when a protected disc is viewed by a PC file manager only the player application program and any files directly associated with the program will be visible.

Each sector on the disc normally contains 2048 bytes of consecutive encrypted digital data, each sector being encrypted with a different unlocking key. This block size is dictated by the "Yellow Book" standard, but in principle data may be encrypted using any convenient block size. Obviously using too large a block size is undesirable as it would result in less variation in the encryption, this should be avoided. The logical sector address (LBA) corresponding to the start of each audio track (LBA-tra) is known to the player application program this data being hidden within the player application program code or at a location on the disc known to the player application program , (hidden within the player code), if the data is located on the disc then the data will its self be encrypted, the information may also be spread over several consecutive or randomly addressed sectors. A particular audio track will normally comprise many thousand consecutive sectors on the disc. The audio data in each of these sectors will be encrypted with a different unlocking key. The player application program contains an algorithm for deriving this unique key from the LBA corresponding to the start of each sector (LBA_{sec}). The skilled person will realize that this algorithm may take a variety of forms, as long as it generates a unique key from the LBA, Thus, when a track is selected the player application program knows the LBA-tra, this is the same as LBA-sec for the first sector of

the track and can derive the key from that LBA-sec to allow data from that first sector to be decrypted. Having read the first sector the player application program knows that the next sector starts at the (LBA-sec) consecutive to the last LBA of the first sector. Knowing LBA-sec the player application program can use the said algorithm to derive the new key and so decrypt data in the second sector. In this way the player application program can decrypt consecutive sectors, each time deriving a new key. This is referred to below as a dynamic key code system.

The dynamic key code system has a number of advantages over known systems. If an unauthorised copier discovers both the LBA-tra and the first key it only allows the first sector (block) of digital audio data to be recovered. The key to the next consecutive sector will normally be completely different. Further, if by some means the consecutive encrypted sectors corresponding to a audio track are copied, for example to a PC hard disc and the player application program is run and directed to the first sector, it will generate wrong keys for each sector because it would need to know original the LBA-sec of the copied material. The sectors occupied on the PC hard disc will almost certainly differ from those on the original disc. Hence, the copied material will not be decrypted by the player software.

Prior to segmentation and encryption of the audio data, this data is preferably compressed using an appropriate compression algorithm.

Preferably, a disc produced according to the invention contains hidden software that is activated when the PC operating system first accesses the storage medium; for example a CD, by reading the directory table of contents data, whereby a memory resident program, hereinafter called "the supervisory program" monitors access to the protected disc. When the disc is removed the supervisory program is removed from the memory of the PC. The supervisory program is also designed to monitor the activity of the disc, including disc

speed, disc access type, (digital or audio) and also ensures reliable playback of the disc content.

In order to be able to monitor the disc activity, the supervisory program must insert its self or part of its self into the operating systems driver chain. Also the supervisory program will be in communication with the player application program that is allowed to "Play" the disc. A driver chain is a computer operating system feature, where an application will communicate with the top part of the chain. This top part of the chain will communicate with the next layer down etc. Until finally the communication will reach, for example, the CD-ROM drive. Information from the CD-ROM drive will travel long the chain in the opposite direction. This mechanism is in place in the operating system in order to present to an application program, a standard way of communicating with a large variety of hardware devices.

The supervisory program inserts its self into this driver chain and can therefore monitor all communications from the application program to the CD-ROM drive. The supervisory program can, for example calculate the average data transfer rate, the type of read operation that is being attempted etc, it also has the ability to identify the disc that is the target of this communication and as a result allow normal operation on a disc that is not protected by the system.

If an operation that is not allowed is attempted then the supervisory program will simply not pass the communication on and will send a fictitious reply to the next higher part of the driver chain and therefore eventually to the application. It may for example chose to simply report an error to the application program or even supply blank or incorrect information. In this way any unauthorized access to a protected disc is blocked.

Sstorage medium according to the invention is only designed to be accessed in one way by a PC; that is using the player application program on the data

session to read and decrypt data therein. If the disc is accessed in any other way the activity will be judged illegal and interventionary action will be taken by the supervisory program. Normally, the supervisory program will stop such activity and the disc will be ejected from the computer drive. This role of the supervisory program will not prevent the copying of an ordinary disc and will not interfere with the general performance and/or activities of the computer.

Thus, if an "illegal" activity such as the digital extraction of disc data to hard disk drive, is detected by the supervisory program that command will be blocked. Likewise, if the player application program is not open, or is closed by the user while the disc is still in the CD-ROM drive then an eject command is sent to the drive.

Access to the first session on the disc, by for example a CD copying utility, will not be allowed by the supervisory program which monitors the position of the read head and can thus identify if data other than session data is being accessed.

If in the unlikely event that a disk copying utility is able to read the first (audio) session of the disc, then the supervisory program will not permit the digital extraction command used by ASPI, ATAPI and other disk command control drivers to be used.

This method monitors the current average disc speed. If the average speed is outside given acceptable parameters then disc access is blocked. Speed monitoring is accomplished by the supervisory program.

When a disc is being played in a PC using the player software the average playback speed of the disc will be very low, since compressed data is being read at real time. Typically data is compressed at a ratio of about 10 to 1, i.e. ten times smaller than the un compressed data; normal playback of the original

data would result in a disc speed of one, therefore the average disc speed when playing the compressed data over the same period of time will be about 1/10 speed in this case.

Because the compressed data is read from the disc in blocks at a high speed (Burst speed), followed by a much longer period of inactivity, speed monitoring will need to measure the average disc speed. The burst speed could in fact be anything up to and including the maximum read speed of the disc, but for very short periods. So called "ripping software" typically will try to copy at the highest speed possible for a sustained period of time. If disc is moving at a high speed on average then access will be blocked (average speeds will need to be calculated over periods in the order of ten seconds). If player application program is not playing the disc then all access to the disc is blocked.

The present invention requires special software to control the disc mastering machine or alternatively a CD-R, CD-RW, DVD-R or DVD-RW disc drive. This will be referred to below as CD Production Software (or CDPS). The CDPS needs to pre-determine the LBA (LBA-tra and LBA-sec) of each sector of data corresponding to any data sessions on the disc. It then selects a particular algorithm and derives the unique encryption key for each sector. Following compression of the audio files and division of the digital data into consecutive segments of audio data, each of these segments is encrypted within a data sector. Thus, when the master disc is produced each sector of data in the data session or sessions, is uniquely encrypted and placed at the pre-determined LBA, so allowing the LBA-sec to be used by a player application program to decrypt and play that sector.

The system of the invention also allows the algorithm that derives a key from a LBA-tra or LBA-sec to be varied if desired for each master disc produced. Advantageously, routine variations in the algorithm used for manufacturing a given master disc can result in completely different keys being derived for a

given LBA. The CDPS will modify the code of the player application program that is also placed on the disc so that it contains the correct algorithm; that is the algorithm used in the encryption step, thus allowing the player application program to decrypt the data session.

CLAIMS

1. A method of manufacturing an optical disc for storing digital data comprising the steps of: (a) segmenting copyright material in digital form into consecutive segments (b) allocating each segment to a sector of the disc (c) pre-determining the position of each sector on the disc and using an algorithm to derive a unique encryption key for each sector according to the logical block address corresponding to the start of each sector (d) encrypting each sector using its unique key, and (d) writing the encrypted data sectors to a disc.

2. Recorded material on an optical disc comprising digital data segmented into consecutive sectors each containing encrypted data, the data in each sector being encrypted using a unique key, the unique key for each sector being dependent upon the logical block address on the disc corresponding to the start of each sector.

3. Optical disc player software containing embedded within its code the logical block address on the disc of the first sector corresponding to a file or track, decryption software operated by a key and an algorithm for determining the unique key for each sector from the logical block address corresponding to the start of that sector.

4. A method of reading encrypting digital data from a disc comprising the steps of (a) decrypting data in consecutive sectors each using a unique key (b) the unique key for each sector being dependent upon the logical block address on the disc corresponding to the start of that sector.

5. A method of preventing a computer copying audio sessions on an optical disc including the steps of (a) describing the audio session as data tracks in the Table of Contents contained within the Q-channel information in the

lead in area of the disc, (b) describing the audio session in the Q-channel data in each sector within the session as audio tracks.

6. A method of monitoring whether a disc according to the invention is being accessed in an authorized way comprising the steps of (a) including software for a supervisory program on the said disc (b) activating this supervisory program when the computer operating system first accesses the disc, (b) insertion of all or part of the supervisory program into the operating systems driver chain that allows two way communication between an application program accessing the disc and the disc drive (d) using the supervisory program to monitor communications between the said application program and the disc drive.

7. A method according to Claim 6 comprising (e) describing an audio session as data tracks in the Table of Contents contained within the Q-channel information in the lead in area of the disc, (f) describing the audio session in the Q-channel data in each sector within the session as audio tracks.

8. A method according to Claim 6 or 7 wherein any application attempting to access data other than the data session or sessions on the disc will be judged illegal and blocked by the supervisory program.

9. A method according to any of Claims 6 to 8 wherein any program other than the player application program accessing the disc will be judged illegal and blocked by the supervisory program.

10. A method according to any of Claims 6 to 9 wherein the current average disc speed is monitored by the supervisory program and if this average speed does not fall within a range determined by the supervisory program blocking access of the application program to the disc by the supervisory program.

11. A method according to any of Claims 6 to 10 where access is blocked by the supervisory program not relaying the communication along the driver chain or relaying a fictitious communication.

12. A method of manufacturing digital data storage medium comprising the steps of: (a) segmenting copyright material in digital form into consecutive segments (b) allocating each segment to a sector of the storage medium (c) pre-determining the position of each sector on the storage medium and using an algorithm to derive a unique encryption key for each sector according to the logical block address corresponding to the start of each sector (d) encrypting each sector using its unique key, and (d) writing the encrypted data sectors to the said storage medium.

13. A method of reading encrypting digital data from a storage medium comprising the steps of (a) decrypting data in consecutive sectors each using a unique key (b) the unique key for each sector being dependent upon the logical block address on the storage medium corresponding to the start of that sector.

14. A method of monitoring whether a storage medium according to the invention is being accessed in an authorized way comprising the steps of (a) including software for a supervisory program on the storage medium (b) activating this supervisory program when the computer operating system first accesses the storage medium, (b) insertion of all or part of the supervisory program into the operating systems driver chain that allows two way communication between an application program accessing the storage medium and a storage medium read/write unit (d) using the supervisory program to monitor communications between the said application program and the storage medium read/write unit.

Abstract

Data Protection System

A method of manufacturing digital data storage medium comprising the steps of: segmenting copyright material in digital form into consecutive segments, allocating each segment to a sector of the storage medium, pre-determining the position of each sector on the storage medium and using an algorithm to derive a unique encryption key for each sector according to the logical block address corresponding to the start of each sector, encrypting each sector using its unique key, and writing the encrypted data sectors to the said storage medium.